IN THE UNITED STATES PATENT & TRADEMARK OFFICE

In re the Application of: **Robert M. BARNHART**

Serial No.: **09/805,279** Art Unit: **3623**

Filed: **March 13, 2001** Examiner: **JARRETT, Scott L.**

For: **VERIFYING A BALLOT USING PUBLIC KEY ENCRYPTION AND DIGITAL SIGNATURES**

FILED ELECTRONICALLY

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This is an Appeal Brief under 37 C.F.R. § 41.37 in connection with the decision of the Examiner mailed on June 4, 2009 setting a three-month period for response to expire on September 4, 2009. A Notice of Appeal was filed on September 4, 2009, setting the period for filing an Appeal Brief to expire on November 4, 2009.

This Appeal Brief fully complies with all provisions of 37 CFR 41.37(c) and each of the topics required by § 41.37 is presented herewith and is labeled appropriately. It is not believed that any additional fees are due, but if so, please charge any deficiency to Deposit Account No. 50-4402.

(1) Real Party In Interest

The real party in interest is Science Applications International Corporation.

(2) Related Appeals And Interferences

Applicants previously filed a Notice of Appeal followed by an Appeal Brief on January 13, 2009 in connection with the decision of the Examiner mailed on June 3, 2008, in response to which the Examiner filed an Examiner's Answer setting forth a new ground of rejection, and prosecution was reopened by Appellants' Reply filed May 4, 2009 to address the new grounds of rejection.

There are no other appeals or interferences related to this case.

(3) Status of Claims

Claims 29-33 are pending and all have been rejected.

Claims 1-28 have been canceled.

No claims have been allowed.

No claims have been withdrawn.

Claims 29-33 are hereby appealed.

(4) Status of Amendments

There are no amendments after final rejection.

(5) Summary of Claimed Subject Matter

Independent claim 29 proposes a method for assisting a user in verifying a cast ballot B_{cast} stored in a server that involves:

- forming a digital signature of B_{cast} using a server side private key $DS(B_{cast}, s)$ (Application [0051] and Figs. 2 and 5) by a first server side computer software application process tangibly embodied in a physical program storage device executable by a server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);

- associating the B_{cast} and $DS(B_{cast}, s)$ with a vote serial number VSN (Application [0053] and Figs. 2, 3 and 5) by a second server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);
- forming a confirmation token, comprising $DS(B_{cast}, s)$ and VSN (Application [0053] and Figs. 2, 3 and 5) by a third server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);
- making the confirmation token available (Application [0053] and Figs. 2 and 5) by a fourth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine to a first client side computer software application process tangibly embodied in a physical program storage device executable by a client side physical computer hardware machine and executing on the client side physical computer hardware machine of a user via a network (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);
- receiving the confirmation token made available to the user (Application [0053] and Figs. 2 and 5) by a fifth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine from a second client side computer software application process tangibly embodied in a physical program storage device executable by the client side physical computer hardware machine and executing on the client side physical computer hardware machine via the network (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);

- extracting $VSN_{\text{received token}}$ and $DS_{\text{received token}}(B_{\text{cast}}, s)$ from the received token (Application [0057] and Figs. 2, 3 and 5) by a sixth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);
- for VSN equal to $VSN_{\text{received token}}$, comparing $DS_{\text{received token}}(B_{\text{cast}}, s)$ and at least one of $DS(B_{\text{cast}}, s)$ and $DS(B_{\text{cast}}, S)$ (Application [0059] and Figs. 2, 3 and 5) by a seventh server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5); and
- determining that B_{cast} is verified (Application [0059] and Figs. 2 and 5) by an eighth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine if the comparison shows equivalence between the data compared (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5).

Independent claim 31 proposes a method for assisting a user in verifying a cast ballot recorded in a server that involves:

- receiving by a first server side computer software application process tangibly embodied in a physical program storage device executable by a server side physical computer hardware machine and executing on the server side physical computer hardware machine at least one set of a cast ballot B_{cast} and a digital signature of B_{cast} formed with the private key of a voter casting the ballot $DS(B_{\text{cast}}, v)$ (Application [0018], [0019], [0024], [0025], [0032]-[0047], [0051] and Figures 2, 3 and 5);
- forming by a second server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer

hardware machine a digital signature of B_{cast} using a server side private key $DS(B_{cast}, s)$ (Application [0018], [0019], [0024], [0025], [0032]-[0047], [0051] and Figures 2, 3 and 5),

- associating B_{cast}, $DS(B_{cast}, v)$, and $DS(B_{cast}, s)$ with a vote serial number VSN (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);
- forming by a third server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine a confirmation token, comprising $DS(B_{cast}, s)$, $DS(B_{cast}, v)$, VSN, and DS(Aggregation, s), where DS(Aggregation, s) is the digital signature of the aggregation of the associated B_{cast}, $DS(B_{cast}, v)$, $DS(B_{cast}, s)$, and VSN (Application [0018], [0019], [0024], [0025], [0032]-[0047], [0053] and Figures 2, 3 and 5);
- making the confirmation token available (Application [0053] and Figs. 2 and 5) by a fourth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine to a first client side computer software application process tangibly embodied in a physical program storage device executable by a client side physical computer hardware machine and executing on the client side physical computer hardware machine of a user via a network (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);
- receiving the confirmation token (Application [0053] and Figs. 2 and 5) by a fifth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine from a second client side computer software application process tangibly embodied in a physical program storage device executable by the client side physical computer hardware machine and executing on the client side physical computer hardware machine via the network (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);

- extracting $VSN_{received\ token}$ and at least one of $DS_{received\ token}(B_{cast}, s)$, $DS_{received\ token}(B_{cast}, v)$, and $DS_{received\ token}(AG, s)$ from the received token (Application [0057] and Figs. 2, 3 and 5) by a sixth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5); and
- for $VSN_{received\ token}$ and the corresponding VSN, comparing by a seventh server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine at least one of $DS_{received\ token}(B_{cast}, s)$ and $DS(B_{cast}, S)$; $DS_{received\ token}(B_{cast}, v)$, and $DS(B_{cast}, v)$; $DS_{received\ token}$(Aggregation, s), and DS(Aggregation, s) (Application [0018], [0019], [0024], [0025], [0032]-[0047], [0059] and Figures 2, 3 and 5);
- determining that B_{cast} is verified by an eighth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine if comparison shows equivalence between the data compared (Application [0018], [0019], [0024], [0025], [0032]-[0047], [0059] and Figures 2, 3 and 5).

Independent claim 33 proposes a method for assisting a user verifying a cast ballot recorded in a server that involves:

- receiving a cast ballot ("Bcast ") (Application [0051] and Figs. 2 and 5) by a first server side computer software application process tangibly embodied in a physical program storage device executable by a server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);
- forming a digital signature of Bcast using a server side private key ("DS(Bcast , s)") (Application [0051] and Figs. 2 and 5) by a second server side computer software application process tangibly embodied in a physical program storage device executable

by the server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);

- associating Bcast and DS(Bcast , s) with a vote serial number ("VSN") (Application [0053] and Figs. 2, 3 and 5) by a third server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5); and
- for VSN, comparing DS(Bcast , s) and DS(Bcast , S) (Application [0059] and Figs. 2, 3 and 5) by a fourth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine (Application [0018], [0019], [0024], [0025], [0032]-[0047] and Figures 2, 3 and 5);
- determining that Bcast is verified by a fifth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine if the comparison shows equivalence between the data compared (Application [0018], [0019], [0024], [0025], [0032]-[0047], [0059] and Figures 2, 3 and 5).

(6) Grounds of Rejection to be Reviewed on Appeal

a) Claims 29-30 and 33 stand rejected under 35 U.S.C. 102(e) as being anticipated by Shrader et al. (U.S. Patent Publication No. 2002/0077887).

b) Claims 31 and 32 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cranor et al. (*Design and Implementation of a Practical Security-Conscious Electronic Polling System*) in view of Shrader.

(7) Argument

The Rejection of Claims 29-30 and 33 Under 35 U.S.C. 102(e) as Anticipated by Shrader is Improper

Independent claims 29 and 33 and claim 30 depending on claim 29 stand rejected as anticipated by Shrader. Shrader does not read on the claimed invention in at least the following respects.

Regarding independent claims 29 and 33:

- Initially, the Examiner asserts in the Final Office Action dated June 4, 2009, page 3, lines 7-page 5, line 19:

> Neither the specification, nor the claimed invention, provide any specificity or clarity as to how or when a vote serial number is assigned/associated to/with a ballot (i.e. the specification provides no clear guidance as to how to interpret the claim "associating the Bcast and DS(Bcast,s) with a vote serial number VSN").
>
> ....
>
> Therefore the examiner is interpreting the claim to encompass associating any unique identifier with a ballot either before or after the voter (user) casts his/her vote ("vote serial number", as defined by the specification,: "Note that the VSN...is ***just an incidental sequence number*** that indicates a vote was delivered in the election" (emphasis added, Paragraph 0054).

As described in the foregoing specification quotation cited by the Examiner, the *VSN* "indicates a ***vote delivered*** in the election." It follows from the past tense usage in the expression, "***vote delivered***", that the VSN cannot be assigned until **after** a vote is "***delivered***". Accordingly, the Examiner's alleged interpretation of the claims to encompass associating any unique identifier with a ballot **either before or after** the voter (user) casts his/her vote is a *per se* mischaracterization of the claim language.

- Based on the foregoing mischaracterization of the claim language, the Examiner further asserts in the Final Office Action dated June 4, 2009, page 5, line 20-page 6, line 7:

> Additionally it is noted that a pre-cast ballot (vote) having an associated vote serial number (e.g. ballot number) retains (remains associated with) the unique identifier even after the ballot has been cast (i.e. once the vote serial number has been assigned to the vote/ballot it remains associated with the ballot before, during and after the user votes using the ballot).
>
> Further it is noted that it is old and very well known in database systems to assign a unique identified (key, primary key, candidate key, unique key), either manually or automatically by the database management system, to all records in a database in fact databases would be unusable without a unique identified associated and assigned to each record as it is stored into the database.

While the use of information uniquely defining a particular database record to locate the stored database record is not disputed, the Examiner's additional allegations simply incorporate and compound the foregoing mischaracterization. For example, the Examiner's allegations regarding "***a pre-cast ballot (vote) having an associated vote serial number (e.g., ballot number)***" and "***vote serial number*** … ***assigned to the vote/ballot*** … ***associated with the ballot before, during and after the user votes using the ballot***" are based on the forgoing mischaracterization of the claims by the Examiner to encompass associating any unique identifier with a ballot **either before or after** the voter (user) casts his/her vote which is belied by the past tense usage in the expression, "***vote delivered***" in the passage quoted by the Examiner in support of such mischaracterization.

- Shrader fails to teach or even suggest a method for assisting a ***user*** in verifying a ***cast*** ballot Bcast stored in a server, as recited in independent claim 29 and similarly in independent claim 33. Neither ***"user"*** nor ***"cast"*** is an optional portion of the claims as implied by the Examiner. Thus, if Shrader does not disclose assisting a "***user"*** in verifying a ***"cast"*** ballot (i.e., a data item that includes actual votes), then Shrader does not anticipate the claims. The written description is clear that the user[1] initiates individual verification of a cast ballot (emphasis supplied):

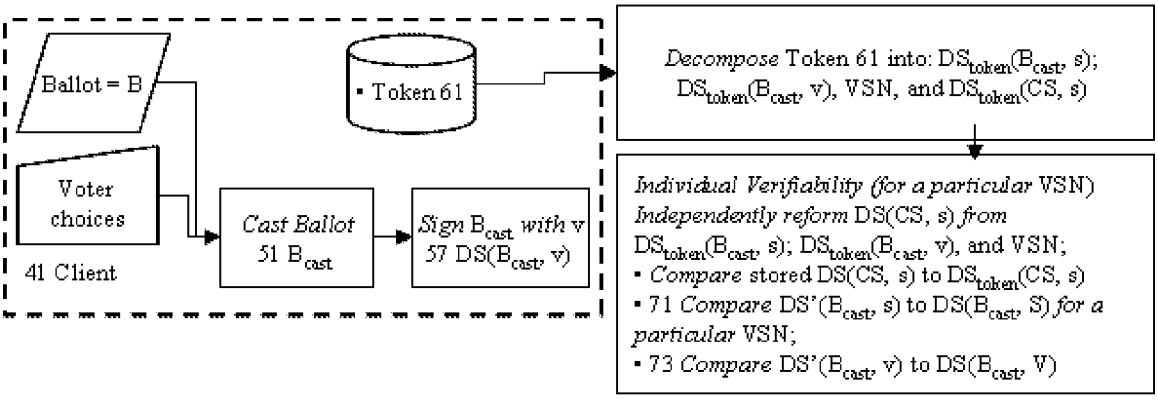
[1] *[0019] ... the terms "individual", "user", "client", and "voter" are used interchangeably, and refer to a person ...*

[0057] Consider now the case where ***an individual would want to connect to the system … to determine if their cast ballot is properly recorded****. In such a case,* ***the individual can present vote confirmation, e.g., token 61****, through a transmission 67 to the server 43 side. …*

[0058] The digital signature on that confirmation can then be recomputed, and it can be verified that the confirmation has not been altered. Having done so, the vote serial number can then be extracted from the confirmation, and the database can be indexed to allow ***reconstruction of the voter's ballot exactly as cast****.*

[0059] Descriptors 71 and 73 illustrate what is known as ***individual verifiability …***

Figure 5, a portion of which is shown here, also shows that *Cast Ballot* includes *Voter choices* and that the user (*Client*) initiates *Individual Verifiability* with a *Token*.



Of the Abstract, [0050]-[0053], [0060],[0063], and Figures 4-8 of Shrader alleged by the Examiner to disclose assisting a ***user*** verifying a ***cast*** ballot, only [0063] in Shrader discloses verification of any sort as hereinafter discussed – and in that case, it is verification **not** involving the ***user*** and explicitly **teaching against** using actual votes from the ballot, i.e., the ***cast*** ballot. Moreover, repeated, detailed examination of Shrader reveals no disclosure whatsoever directed to assisting a ***user*** in verifying the votes of a ***cast*** ballot.

- Shrader fails to disclose forming a digital signature of $\boldsymbol{B_{cast}}$ using a ***private key of the server*** $DS(B_{cast}, s)$, as recited in independent claims 29 and 33. The Examiner alleges in the Final Office Action dated June 4, 2009, page 14, lines 17-21 that this limitation is

disclosed in [0063] and Figures 7-8 element 72 of Shrader, specifically citing the underlined portion of the following passage:

> *[0063] … The voting tabulator receives the encrypted voting information from the voting entity 69 and decrypts the encrypted voting information with the tabulator's own private key 70, to get the votes and the encrypted electronic ballot. … The voting tabulator signs, encrypts and sends the encrypted electronic ballot to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and signed with the voting tabulator's private key.*

However, according to the non-underlined portion of the above passage, "voting information" includes "votes" ***and*** "encrypted electronic ballot." Shrader's "encrypted electronic ballot" does not contain votes. In the present application, B_{cast} includes votes (see, e.g., Figure 5, *Voter choices*). It is clear that instead of forming a digital signature of B_{cast}, as recited in claims 29 and 33, Shrader simply forms a digital signature of the ballot, B. Further, in Shrader the digital signature of the ballot is encrypted with the public key of the mediator/server, i.e., DS(B, S) in the notation of the application, not DS(B_{cast}, s) as recited in claims 29 and 33. Thus, Shrader discloses the wrong data encrypted with the wrong key.

- Shrader likewise fails to disclose associating the B_{cast} and DS(B_{cast}, s) with a vote serial number VSN, as recited in independent claims 29 and 33. In alleging that this limitation is taught by Shrader, the Examiner, at page 14, line 22 of the Final Office Action dated June 4, 2009, again mischaracterizes the claim language as "associating (storing, linking, relating, etc.) the (cast) ballot, the voter's digital signature of the ballot with a ballot number …." On the contrary, DS(B_{cast}, s) is not the "voter's digital signature of the ballot" – that would be DS(B, v) for the voter's private key, or DS(B, V) for the voter's public key. Instead, DS(B_{cast}, s) is the digital signature of B_{cast} (which includes actual votes) using a private key of the server. The specification clearly describes the notation used in the claims as follows:

  > *[0052] Throughout this disclosure in labels such as DS(...,C) or DS(...,c), an upper case letter in the second position means a public key, and a lower case letter means a secret or private key, ...*

[0053] ... Specifically, the ***server's signature of the cast ballot DS(B_{cast}, s)*** *53.*

Further, *VSN* is not the ballot number. While the specification notes that *VSN* can be ***like*** a ballot serial number, as previously noted herein, the specification clearly describes it as follows (emphasis added):

> *[0053] ... Note that the VSN ... is just an incidental sequence number that indicates* ***a vote delivered*** *in the election.*

According to Shrader [0061], [0063], Figures 5-6 elements 57 and 58, and Figure 8 element 71, cited by the Examiner as disclosing associating the B_{cast} and DS(B_{cast}, s) with a vote serial number VSN, as recited in independent claims 29 and 33, the elements to be associated do not exist until after a voter's choices have been made; each element requires a voter choices; and voter choices do not exist in Shrader until [0062] and Figure 7. Thus, it is patently impossible for Shrader [0061], and Figures 5, 6 to disclose the yet-to-exist elements (B_{cast}, DS(B_{cast}, s), and VSN), which leaves only Shrader [0063] and Figures 7 and 8 to disclose the elements and their association. Those portions of Shrader address verification as follows (**bold** emphasis added to show where the reference not only fails to disclose the claim limitation, but also teaches away from it):

> *[0063] … The message that the tabulator sends to the mediator is a verification message.* ***The verification message does not contain the actual votes from the ballot****, since the voting must be anonymous. Instead, the verification message contains identifying ballot information such as the* ***ballot number****, to ensure that it was issued by the mediator and has not been previously used.*

Notice that Shrader teaches away from using "actual votes" in its verification message and instead uses a **ballot number** which exists **before** a vote instead of a **vote serial number** which applicant's claimed invention assigns **after** a vote (see, e.g., Application [0054] quoted above).

- Further, Shrader fails to teach forming a confirmation token, comprising DS(B_{cast}, s) and VSN, as recited in independent claim 29. In alleging that this limitation is taught by Shrader, at page 15, line 1 of the Final Office Action dated June 4, 2009, the Examiner once again mischaracterizes the claim language as "forming a message (confirmation, string, receipt, acknowledgement, token, etc.) comprising a system's **digital signature of**

the ballot and the **ballot number**." First, claim 29 recites a digital signature of the cast ballot (i.e., B_{cast}) instead of the ballot B as mischaracterized by the Examiner. Second, claim 29 recites use of a VSN instead of a ballot number as mischaracterized by the Examiner. The differences contribute to distinguishing the claim from the reference. In addition to mischaracterizing the language of claim 29, the Examiner ignores the disclosure of Shrader [0063] that **excludes** vote (i.e., part of B_{cast}) from the message:

> *[0063] … **The verification message does not contain the actual votes from the ballot**, since the voting must be anonymous. …*

It is abundantly clear that Shrader does not form a confirmation token comprising a vote and vote serial number.

- Additionally, Shrader fails to disclose making the confirmation token available to a **user** and/or receiving a confirmation token made available to a **user**, as recited in independent claim 29. In fact, the Examiner simply ignores the fact that the confirmation token is to be made available to the user, alleging only at page 15, lines 5-6 of the Final Office Action dated June 4, 2009 that Shrader discloses "making the message available (verification message exchanged between tabulator to **mediator**; Paragraphs 0061, 0063, Figures 7-8)". As noted above, Shrader does not form a confirmation token. Further, Shrader's mediator, **a server process**, is **not** a **user** as defined in the present application:

  > *[0019] ... the terms "individual", "user", "client", and "voter" are used interchangeably, and refer to a person ...*

- In addition, Shrader fails to teach the comparison and verification recited in independent claims 29 and 33. Specifically, Shrader fails to teach comparison between $DS_{\text{received token}}$ (B_{cast}, s) (the received-token version of the digital signature over the cast ballot containing votes using the private key of the server) and one of DS (B_{cast}, s) (the digital signature over the cast ballot containing votes using the private key of the server as stored on the server), or DS (B_{cast}, S)(the digital signature over the cast ballot containing votes using the public key of the server as stored on the server). As previously noted, Shrader [0061]-[0063] and Figures 7, 8 alleged at page 15, lines 16-18 of the Final Office Action dated June 4, 2009 by the Examiner to teach the comparison and verification recited in

independent claims 29 and 33, does not disclose any sort of verification until the middle of Shrader [0063]. There, Shrader teaches checking to see if ballot number (not a VSN, and most assuredly not a data item including B_{cast}) has already been used. This is **not** a comparison of digital signature over a data item containing the votes, which comparison is required by the claims.

Applicants' identical invention is shown nowhere in Shrader in complete detail as contained in independent claims 29 and/or 33 or with the elements arranged as required by claims 29 and/or 33 (see, Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) and In re Bond, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990)). Consequently, Shrader does not disclose nor even suggest the required combination of limitations of independent claims 29 and/or 33. Because each and every element as set forth in independent claims 29 and/or 33 is not found, either expressly or inherently in Shrader, the Examiner has failed to establish a *prima facie* case of unpatentability. See Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628 (Fed. Cir. 1987); see also MPEP §2131.

Regarding claim 30 depending on claim 29, the Examiner has failed to establish the required *prima facie* case of unpatentability for independent claim 29, and similarly has failed to establish a *prima facie* case of unpatentability of claim 30 depending on claim 29, and which recites further specific elements that have no reasonable correspondence to the reference in at least the following respects:

- Claim 30 depending on claim 29 recites the addition of elements to the *confirmation token* of claim 29 before it is made available to a user and after receiving the *confirmation token* from a user, extracting those additional elements, and thereafter verifying a cast ballot upon the additional condition that the additional elements of the *confirmation token* are equivalent to the version of those elements stored on the server for that VSN. The Examiner alleges at page 18, lines 1-5 of the Final Office Action dated June 4, 2009 that Shrader [0061]-[0063] and Figures 7, 8 discloses the further specific elements recited in claim 30:

> *... the message (confirmation token, received token) further comprises the system's digital signature of the*

ballot and ballot number (aggregation; Paragraphs 0060-0062; Figure 2, Certificate No.)

As repeatedly pointed out, the specific claim language requires the digital signature of a data item containing the cast ballot and the use of a vote serial number (VSN) instead of a ballot number. The claim language is again mischaracterized by the Examiner. As also pointed out, while the Examiner cites Shrader [0060]-[0062] and Figure 2 as disclosing the formation and use of a token used for verification, Shrader does not disclose any sort of verification until [0063]. Further, Figure 2 is an illustration of a paper voter registration "certificate" that is in no way whatsoever connected to verification of a cast ballot. The remainder of the claim 30 requires extracting information that Shrader does not, from a token that Shrader does not form or receive, in order to provide individual verification (a function that Shrader does not provide).

The Rejection of Claims 31 and 32 Under 35 U.S.C. 103(a) Over Cranor and Shrader is Improper

Independent claim 31 and claim 32 depending on claim 31 stand rejected as obvious over Cranor and Shrader. The proposed modification of Cranor in view of Shrader lacks one or more limitations recited in each of the claims, and there is inadequate articulated reasoning with rational underpinning to support the Examiner's legal conclusion of obviousness in at least the following respects:

- Cranor fails to teach or suggest "receiving…at least one set of: a cast ballot B_{cast} and a digital signature of B_{cast} formed with the private key of a voter casting the ballot $DS(B_{cast}, v)$" and/or "forming…: a digital signature of B_{cast} using a server side private key $DS(B_{cast}, s)$", as recited in independent claim 31. On the contrary, while Cranor recites "the voter to prepare a voted ballot, encrypt it with a secret key, and blind it" (Cranor, par. 2, p. 5), Cranor fails to disclose which secret key is used for encryption. Instead of "a digital signature of the B_{cast} formed with the private key of a voter casting the ballot $DS(B_{cast}, v)$" and "forming…: a digital signature of Bcast using a server side private key $DS(B_{cast}, s)$" (i.e., the digital signatures are created using different private keys, the voter's private

key and the server's private key), as recited in claim 31, Cranor simply recites a secret key and without reciting the possessor of the private key.

- Instead of "associating B_{cast}, $DS(B_{cast}, v)$, and $DS(B_{cast}, s)$ with a vote serial number VSN;" as recited in independent claim 31, Cranor discloses voter registration without addressing a cast ballot. (Cranor, pars 3 and 4, p. 7)

- Neither does Cranor teach or suggest the confirmation token comprising "$DS(B_{cast}, s)$, $DS(B_{cast}, v)$, VSN, and DS(Aggregation, s), where DS(Aggregation, s) is the digital signature of the aggregation of the associated B_{cast}, $DS(B_{cast}, v)$, $DS(B_{cast}, s)$, and VSN" where VSN is the vote serial number, as recited in independent claim 31. On the contrary, Cranor fails to teach or suggest which keys are used to form the digital signatures. (Cranor, par 2, p 5, last par, p 7; pars 1-4, p 8, and Fig 1). For example, Fig 1 does not teach or suggest which keys are used to form the digital signatures. Regardless, there is no hint of teaching or suggestion in Cranor of forming a confirmation token comprising "$DS(B_{cast}, s)$, $DS(B_{cast}, v)$, VSN, and DS(Aggregation, s)", as recited in claim 31.

- For same reasons set forth herein with respect to the discussion of independent claims 29 and 33, Shrader fails to remedy the deficiencies of Cranor. Similar to the rejection of independent claims 29 and 33, the Examiner continues to mischaracterize the claims at page 20, line 13-page 22, line 17 of the Final Office Action dated June 4, 2009, for example, by substituting "ballot" (e.g., a list of candidates for each position in an election) for ***"cast ballot"*** (B_{cast}, which includes voter's choices); by substituting "voter's identification number" and "ballot number" for ***"vote serial number (VSN)"***; by substituting "entity, … system, subsystem, third party" for ***"user;"*** and by neglecting to account for the inclusion of the digital signature of the cast ballot using the server's private key as an element of the association called for in Claim 31. There is no support for interpreting the claim language in this fashion. Both Shrader and Cranor clearly distinguish: **a)** between empty ballots and choices/votes/cast ballots; **b)** between voter ID numbers, uncast ballot numbers, and number assigned to actual votes; and **c)** between the system and users/voters. In fact, as mentioned above, Shrader even **teaches against**

equating an empty ballot with a cast ballot. It is axiomatic that a *prima facie* case of obviousness cannot be made while neglecting to account for all the elements of the claim.

Consequently, the claimed combinations recited in independent claim 31 are not taught or suggested by Cranor and/or Shrader, either separately or in combination with one another. Because the cited references, either alone or in combination, do not teach the limitations of independent claim 31, the Examiner has failed to establish the required *prima facie* case of unpatentability. See In re Royka, 490 F.2d 981, 985 (C.C.P.A., 1974) (holding that a *prima facie* case of obviousness requires the references to teach all of the limitations of the rejected claim); See also MPEP §2143.03.

Regarding claim 32 depending on claim 31, the Examiner has failed to establish the required *prima facie* case of unpatentability for independent claim 31, and similarly has failed to establish a *prima facie* case of unpatentability of claim 32 that depends on claim 31, and which recites further specific elements that have no reasonable correspondence to the references in at least the following respects:

- Claim 32 depending on independent claim 31 requires determining whether a confirmation token has been modified since its formation. Cranor does not address determining whether a token has been modified (Cranor, par 2, p. 5; last par, p. 7; and pars 1-4, p. 8).

(8) Conclusion

For at least the reasons given above, the rejection of claims 29-33 is improper. Applicants respectfully request the final rejection by the Examiner be reversed and claims 29-33 be allowed.

Respectfully submitted,

Date: November 2, 2009

By: */John M. Harrington, Reg. #25,592/*
John M. Harrington
(Reg. No. 25,592)

KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 737-0500

(9) Claims Appendix

29. A method for assisting a user in verifying a cast ballot B_{cast} stored in a server, the method comprising:

forming a digital signature of B_{cast} using a server side private key $DS(B_{cast}, s)$ by a first server side computer software application process tangibly embodied in a physical program storage device executable by a server side physical computer hardware machine and executing on the server side physical computer hardware machine;

associating the B_{cast} and $DS(B_{cast}, s)$ with a vote serial number VSN by a second server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine;

forming a confirmation token, comprising $DS(B_{cast}, s)$ and VSN by a third server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine;

making the confirmation token available by a fourth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine to a first client side computer software application process tangibly embodied in a physical program storage device executable by a client side physical computer hardware machine and executing on the client side physical computer hardware machine of a user via a network;

receiving the confirmation token made available to the user by a fifth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine from a second client side computer software application process tangibly embodied in a physical program storage device executable by the client side physical computer

hardware machine and executing on the client side physical computer hardware machine via the network;

extracting $VSN_{\text{received token}}$ and $DS_{\text{received token}}(B_{\text{cast}}, s)$ from the received token by a sixth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine;

for VSN equal to $VSN_{\text{received token}}$, comparing $DS_{\text{received token}}(B_{\text{cast}}, s)$ and at least one of $DS(B_{\text{cast}}, s)$ and $DS(B_{\text{cast}}, S)$ by a seventh server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine; and

determining that B_{cast} is verified by an eighth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine if the comparison shows equivalence between the data compared.

30. The method of Claim 29 wherein:

the confirmation token further comprises a digital signature of an aggregation comprising the associated B_{cast} and VSN using the server side private key DS(Aggregation, s);

extracting $DS_{\text{received token}}$ (Aggregation, s) from the received token; and

B_{cast} is verified only upon the additional condition that $DS_{\text{received token}}$ (Aggregation, s) is equivalent to DS(Aggregation, s).

31. A method for assisting a user in verifying a cast ballot recorded in a server, the method comprising:

receiving by a first server side computer software application process tangibly embodied in a physical program storage device executable by a server side physical computer hardware machine and executing on the server side physical computer hardware machine at least one set of:

a cast ballot B_{cast} and

a digital signature of B_{cast} formed with the private key of a voter casting the ballot $DS(B_{cast}, v)$;

forming by a second server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine:

a digital signature of B_{cast} using a server side private key $DS(B_{cast}, s)$,

associating B_{cast}, $DS(B_{cast}, v)$, and $DS(B_{cast}, s)$ with a vote serial number VSN;

forming by a third server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine a confirmation token, comprising:

$DS(B_{cast}, s)$, $DS(B_{cast}, v)$, VSN, and DS(Aggregation, s),

where DS(Aggregation, s) is the digital signature of the aggregation of the associated B_{cast}, $DS(B_{cast}, v)$, $DS(B_{cast}, s)$, and VSN;

making the confirmation token available by a fourth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine to a first client side computer software application process tangibly embodied in a physical program storage device executable by a client side physical computer hardware machine and executing on the client side physical computer hardware machine of a user via a network;

receiving the confirmation token by a fifth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine from a second client side computer software application process tangibly embodied in a physical program storage device executable by the client side physical computer hardware machine and executing on the client side physical computer hardware machine via the network;

extracting $VSN_{\text{received token}}$ and at least one of $DS_{\text{received token}}(B_{\text{cast}}, s)$, $DS_{\text{received token}}(B_{\text{cast}}, v)$, and $DS_{\text{received token}}(AG, s)$ from the received token by a sixth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine; and

for $VSN_{\text{received token}}$ and the corresponding VSN, comparing by a seventh server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine at least one of:

$DS_{\text{received token}}(B_{\text{cast}}, s)$ and $DS(B_{\text{cast}}, S)$;

$DS_{\text{received token}}(B_{\text{cast}}, v)$, and $DS(B_{\text{cast}}, v)$;

$DS_{\text{received token}}(\text{Aggregation}, s)$, and $DS(\text{Aggregation}, s)$;

determining that B_{cast} is verified by an eighth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine if comparison shows equivalence between the data compared.

32. The method of Claim 31 further comprising:

if comparison shows equivalence between $DS_{received\ token}$(Aggregation, s), and DS(Aggregation, s), determining that the received confirmation token has not been modified since its formation.

33. A method for assisting a user verifying a cast ballot recorded in a server, the method comprising:

receiving a cast ballot ("Bcast ") by a first server side computer software application process tangibly embodied in a physical program storage device executable by a server side physical computer hardware machine and executing on the server side physical computer hardware machine;

forming a digital signature of Bcast using a server side private key ("DS(Bcast , s)") by a second server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine;

associating Bcast and DS(Bcast , s) with a vote serial number ("VSN") by a third server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine; and

for VSN, comparing DS(Bcast , s) and DS(Bcast , S) by a fourth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side physical computer hardware machine;

determining that Bcast is verified by a fifth server side computer software application process tangibly embodied in a physical program storage device executable by the server side physical computer hardware machine and executing on the server side

physical computer hardware machine if the comparison shows equivalence between the data compared.

(10) Evidence Appendix

There is no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, 1.132 and no other evidence entered by the examiner and relied on by appellant in the appeal.

(11) Related Proceedings Appendix

Applicants previously filed a Notice of Appeal followed by an Appeal Brief on January 13, 2009 in connection with the decision of the Examiner mailed on June 3, 2008, in response to which the Examiner filed an Examiner's Answer setting forth a new ground of rejection, and prosecution was reopened by Appellants' Reply filed May 4, 2009 to address the new grounds of rejection.

There are no other decisions rendered by a court or the Board in any other appeals or interferences related to this case.